Efficient Encryption Scheme for Secure Data Storage in Cloud Computing

SHORT SYNOPSIS

Submitted in partial fulfillment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

To

Manav Rachna International Institute of Research and Studies

(Deemed to be University)

By

Pronika
Registration Number:16/Ph.D/031

Under the supervision of

Dr. S.S. Tyagi
Professor, Computer Science & Engineering

FACULTY OF ENGINEERING AND TECHNOLOGY

MANAV RACHNA INTERNATIONAL INSTITUTE OF RESEARCH & STUDIES

SECTOR-43, SURAJKUND –DELHI ROAD, FARIDABAD – 121001

FACULTY OF ENGINEERING AND TECHNOLOGY

Certificate

I hereby declare that the short synopsis "Efficient Encryption Scheme for Secure Data Storage in Cloud Computing" being submitted in partial fulfillment of the requirement for the degree of Doctor of Philosophy in Computer Science & Engineering under faculty of Engineering And Technology of Manav Rachna International Institute of Research & Studies, Faridabad during the academic year 2019.

It is a bona fide record of original work carried out under the supervision of Dr. S. S. Tyagi and has not been submitted in full or part to any other university or institute for degree or diploma. Further, it is certified that short synopsis is plagiarism free and proof has been submitted.

Pronika

16/Ph.D/031

Signature of the Supervisor

Dr. Shyam Sunder Tyagi

Professor-CSE

Faculty of Engineering & Technology

Manav Rachna International Institute of Research &Technology

(Chairman, DRC)

Chairperson, CDP

CONTENTS

S. No.	Description	Page No.
1	Introduction	1-6
	1.1 Cloud Computing	
	1.2 Cloud Computing Security	
2	Literature Review	7-11
3	Description of Broad Area	12-13
	3.1 Gaps in the Research	
4	Objectives of the Research	14
5	Methodology to be adopted	14
6	Expected Outcome of the Research	15
7	References	16-18

ABSTRACT

Cloud computing (CC) is an expanding computing standard. It gives enormous measure of processing and space to cloud users provisioned as a facility over the web in a pay per use model, where the users or clients pay just as indicated by the use of their service. Distributed storage is main significant facility which enables the users to save their information from nearby computing infrastructure to the isolated cloud. Putting away the information in isolated cloud storage has turned into a pattern and progressively useful now a days. The clients can store a lot of information in it at a moderately lesser cost. Subsequently the key purpose for utilizing cloud computing is cost effectiveness, which is especially valid for little and middle-sized organizations. By putting away their information in the cloud, the clients can ignore the starting savings of costly framework arrangement, enormous equipment and day by day increasing cost.

The unique element of the cloud moreover presents numerous security inspiring design concerns, which should be obviously assumed and settled. The main significant security viewpoints that should be addressed to guarantee the availability, integrity and confidentiality of the information saved in the cloud. Since, users don't have command above the information, the current cryptography systems can't be accepted directly for this reason. In this way, an effective and proficient facility is mandatory to the users to check if the saved information in cloud is kept up or cooperated. The recently planned protocols for isolated information checking frequently give very week declaration to the users about security of their information put away in cloud. This is because of its multitenancy, dependency on public internet, external data storage lack of control features. When allowing for the security, it still requests some additional security methods. It includes basically a common methodology of encryption.

There are a limited policies and methods used to preserve the security of information. This research work focus on data storage at many stages. At each point it improves its security. Our aim is to accomplish security and integrity of data storage. This specifies an essential point for cloud storage providers to accept policies for outsourced data in order to gain trustworthiness from clients. Proof of retrievability, proof of ownership, and provable data possession are major cloud integrity systems available to ensure availability and data integrity for data storage. Proof of retrievability ensures data integrity with error correcting codes to recover from data corruption which was a limitation for other two schemes. Hence, the major focus of this work would be to

improvise proof of retrievability scheme by efficiently integrating proof of retrievability and proof of ownership schemes and to work upon assured deletion problem.

Key words: Cloud computing, cloud storage, data security, encryption scheme, data storage, data integrity.

1. Introduction

1.1 Cloud Computing

"Cloud" is an aggregate word for countless improvements and potential effects. It's everything but a formation however an improvement or development, yet even more a "down to earth advancement", joining a few earlier inventions into somewhat new and considerable. Cloud computing combines a couple of available advances like high information transmission frameworks, virtualization, time sharing, and program interfaces. Cloud is an Internet-based development, where shared assets, for example programming, storage, data and platform are given to the clients for their interest. It is a developed stage for sharing assets that consolidate programming, frameworks, applications, and business structures. Cloud computing is a virtual pool of registering resources. Cloud computing framework is accessed to utilizing system which gives programming, equipment, preparing power and so forth to the client when request is created. It is a basically a pool of resources which provide to customers through web.

Cloud computing gets its name as an illustration for the Internet. Fundamentally, cloud computing is a build that enables us to get to applications that really dwell at an area other than our PC or other web associated gadget. The excellence of cloud computing is that another organization has your application (or suite of utilizations). This implies they handle the expense of servers, they deal with the product refreshes and relying upon your agreement you pay for the service.

The term cloud computing was first utilized in a scholarly setting in 1997 by Prof. Kenneth at the Informs Conference at Dallas as "a registering worldview where the limits of processing will be controlled by financial method of reasoning instead of specialized points of confinement".

It is a model for enabling supportive, on-request framework access to a typical pool of processing resources (e.g., frameworks, servers, applications, storage and administrations) that can be immediately provisioned and released with minimum organization efforts or service

provider collaboration. The on-request self-service, pay-by-use environment of cloud computing is moreover an expansion of built up patterns. The on-request nature of distributed computing serving to supports the act and capacity parts of service-level destinations. The on-request service facility of cloud computing lets associations to make versatile situations to broaden and contract supported the business and mark execution parameters.

Cloud computing include five fundamental characteristics, four deployment models and three service models. The characteristics of cloud computing are:

1. Broad Network System

2. Resource Pooling

3. On request self service

4. Rapid flexibility

5. Measured Service

Private cloud, public cloud, community cloud and hybrid cloud are different types of deployment models of cloud computing and Cloud Infrastructure as a service, Cloud Software as a service and Cloud Platform as a service are types of service models of cloud computing.

Virtualization permits a dynamic datacenter any place servers give a pool of resources that are controlled as required, and the relationship of utilizations to process or capacity, and system assets changing all around progressively to fulfill every remaining task at hand and business requests.

Cloud is a rising innovation that clears a route for endless enhancements and potential results. It's definitely not an improvement, anyway to a more noteworthy degree a practical progression that joins various existing creations bringing forth another and convincing innovation. Without cloud innovation an association, regularly has its very own server farms and servers where it runs its very own applications (manufactured or bought). In a conventional server farm condition a server that runs an application today will in all probability be running a similar application tomorrow. In the event that a conceivable change is required to move the application starting with one machine then onto the next an earlier permission from the specialists should be

mentioned, which implies that applications can't be powerfully assigned to the servers that have the most limit accessible. Therefore, a large portion of the resources remain underutilized. Accordingly, the servers must be physically arranged in this steady state condition.

1.1(a) Services

It is basically an idea of having the option to utilize reusable, fine-grained parts over a merchant's system. This is generally referred to "as a service".

Contributions with a service as an addition incorporate:

- Low obstructions to passage, making them accessible to private ventures
- Large versatility
- Multitenancy, which enables resources to be shared by numerous clients.
- Device independent, which enables clients to get to the frameworks on various equipment.

Infrastructure as a service (Iaas): It is the product that purchasers use to store, process, and organize the different essential figuring resources, convey and execute working frameworks or applications, etc. Customers can send and run handling, storage, organizing, and other fundamental figuring assets freely, without the need to buy network devices, for example, storage and servers. They can't control or control the fundamental framework, yet can control working frameworks, storage devices, and conveyed applications.

It gives capacity to the purchasers to hire infrastructure segments, for example, servers, storage and organizes and empowers them to convey and track encoding including occupied framework and applications. The customer contracts these resources as an administration dependent on requirements and pays just for utilization.

Platform as a service (PaaS): It gives the capacity to clients to send and make cloud foundation to customers, or to utilize programming languages, libraries, and administrations. Clients don't have to oversee and switch the cloud structure, including the framework, servers, working systems or limit, anyway need to control the upper application association and application

encouraging condition. PaaS can be described as an improvement condition gave as a service by the cloud provider. The buyers utilize the phases that include supervisor, produce, compiler and send abilities to develop their applications. Exactly when purchasers form their applications to continue running over the PaaS provider's product stage, versatility and flexibility is guaranteed direct by the PaaS arrange.

Software as a service (SaaS): SaaS is a model that gives software through the Internet. Rather than obtaining software, clients can utilize the Web-based software to deal with their business exercises without keeping up the product. The specialist organization oversees and keeps up the product, for some private companies, SaaS is the most ideal approach to embrace cutting edge innovation, which takes out the requirement for organizations to purchase, assemble and keep up foundation and applications.

It is a capacity given to the purchaser to use provider's applications running in a cloud framework. SaaS is at the upper most layer of distributed processing stack which is used by the end customer. In SaaS model applications for example, Email, texting services given by the provider. The cloud provider will have and manage the required foundation and balance the applications which help these services.

1.2 Cloud Computing Security

Cloud computing offer programming applications, infrastructure and system benefits. The administrations of cloud are facilitated in a server farm which can be utilized by clients with the assistance of system network. Henceforth, it has a necessity for giving integrity and security in cloud assets. Maximum security devices have a finite pace of disappointment, and the interference goes with progressively and difficult strategies; the security disappointment duties are increase rapidly.

At the present time, online cloud organizations are commonly utilized for giving an enormous capacity of extra room and best of the processing stages. Consequently, there is a requirement for giving security and trustworthiness in cloud assets. By and large, cloud foundations are much strong and incredible than ordinary processing stages. Regardless, unapproved access and malicious clients have seen to be an important concern in checking the cloud framework. These undesirable clients may change or remove even additional criticalness information being put

away in the cloud foundation. These days a wide extent of accessibility and dependability parts are merged into the cloud administrations for giving the security in cloud assets. Likewise, on interest cloud administrations are given to clients over the web. In this manner, the undesirable cloud administrations can be detached by the customers that would decrease the full scale price. These days, various cloud specialist organizations are significantly giving a scope of interest by providing computing devices, network, storage space etc. The presentation of cloud associations can be sketched out with the help of many execution assessment take in considerations, like the reaction time of the virtual machine, sitting tight time for getting to the cloud benefits, the price of each cloud benefits, and so forth. Cloud specialist co-ops have built up various protocols for getting to the cloud assets. In any case, they give fewer security administrations to the end clients.

The data encryption is classified into different kinds; anyway various sorts are not strong. In last decades, 64-piece encryption strategies are seen to be a hearty response for anticipate the more critical data. Later 128-piece encryption strategy is presented with clarify the issues exist in 64-piece encryption strategy. From that point, the Advanced Encryption Standard (AES) encryption system is presented for approving a limit of 256-piece with everything taken into account. All the more regularly, information encryption is divided into symmetric and unbalanced or asymmetric information encryption calculations. In symmetric key systems, an ensured key is created and shared between the sender and authority. The key occupation of this key is to encode and decode the content. Diffie-Hellman key and RSA strategies not related to symmetric key encryption procedures. In these key procedures, two or three private key and an open key are made to encode and decode the content. Mainly, the open key is utilized by users or anyone to encode the information. The secure key is utilized by the director to unscramble the information. These days, information encryption techniques are broadly utilized for encoding and decoding the information put away in the cloud storage.

According to the encoding, the information or data change into different form which can be access by authorized person. With the help of encoding, American Standard Code for Information Interchange (ASCII) changes the information into important form that can be beneficial for customer. The ASCII comprises the scope of not printable and up print strategies that order the upper case, lower case alphabets, digits, and images. For some circumstances, a

particular value is utilized for encoding the input information. To defeat the encryption problem, an assortment of steganography procedures is introduced as of late.

The steganography strategies are utilized to impart the information between different users where the information correspondence isn't comprehended by outsiders. In this technique, secret information is secured with the assistance of different kinds of pictures, sound, and video. These days, distributed computing clients have begun utilizing of different techniques like steganography between users for secure transmission of information. For secure data utilizing, steganography strategies are put away at all important information or data in the form of file in cloud.

Cloud storage has so many benefits for storing the data on the web like pay according to your use. It is a cheap service provided by service provider. From last some years, when information it may be personal or business related when saved to public cloud for persistent capacity. The owner of the information which is stored on public cloud is not trusted and the data should not be given to cloud supplier without the knowledge of the owner. Numerous capacity system having access control of dominated server like secure key and certification related confirmation. They too much believe the supplier to ensure their personal information will be secured in the cloud server. The representatives of supplier can use any materials without the permission of owner's access policy. Data owner who put away their record on servers still need to balance the entrance and keep the information secret against the malicious users and cloud supplier. The method of encryption and decryption is not securing the information all the time.

For using the secrecy ensure, data owner can encrypt the documents and put an entrance strategy only the authorized customer can found the record. Cloud computing is another however slow development model of big business IT foundation that gives superb applications and administrations. The clients can redistribute their nearby unpredictable information framework into the cloud to balance a methodology from the overhead and local storage. Be that as it may, the security of outsourced information can't be ensured, as the Cloud Service Provider (CSP) has entire control of the information. Along these lines, it is important to encode information before outsource them into cloud to secure the protection of sensitive information. It gave a secure protection preserving redistributed classification in distributed computing. Be that as it may, encryption for redistributed information can secure protection against unapproved practices; it

additionally makes successful information usage, for example, search over encrypted information, and a very difficult issue.

2. Literature Review

(Mahmood 2011) Author analyzed various issues of information in the cloud and talked about Cloud processing deals for an irregular state of information portability. Exactly when a venture has some delicate information that is kept on a storage related device in the cloud, they might need to know its area. He broke down that web services like AWS give a decision inside its Simple Storage Service (S3) pack to empower customers to decide the geographic region for the capacity and area of information. It is like manner gives affirmation that the information won't leave the client chose region and Microsoft declared that its Windows Azure framework would give clients an alternative to show geographic areas where the client information is to be taken care of. This paper essentially centers on the issues related to data, cost, storage with its location and security.

(Ng, W.K., Wen, Y. and Zhu, H., 2012) Authors discussed the private data deduplication in which a user or customer has a private data and it shows to server with the string of the data in brief form. It's basically a customer duty that he should not disclose to server regarding their personal data. Authors analyzed private deduplication method which include cryptography standard and it shows that simulation based system which include hash function are more secure that is collision resistant but discrete algorithm is complex.

(Sun, Zhang and Zhu 2014) Authors analyzed when normally encrypt the data it faced many key management issues and can't help complex necessity for example fine grained approval, parallel alternation and query. Authors suggested fully homomorphic encryption strategy for data confidentiality, which can work for any activity that can do it in clear content and not taking the procedure of decrypting the data. For greater flexibility and upgraded security, hybrid techniques that consolidate numerous encryption algorithms, for example, triple data encryption standard, random number generator and RSA has been purposed.

According to them RSA is valuable for building up secure correspondence with the help of digital signature while triple data encryption standard is helpful for block data which was encrypted. The homomorphic encoding calculation is inefficient, a light weight component

purposed for database encryption known as transposition, substitution, folding and shifting (TSFS) calculation. In this paper authors purposed various procedures for information assurance and accomplish most abnormal amount of information security in the cloud but these methods become more effective when the gaps in the study can be filled.

(Mahalle & Shahade 2014) Authors purposed a hybrid encryption system utilizing AES and RSA algorithm in this paper. High Security of content records and make the entrance of unique document by intruders close to impossible is given by utilizing hybrid encryption calculation. Be that as it may, just a single Drawback here is the execution time. The time taken to execute the entire procedure is higher than different strategies.

(Hussain & Ashraf 2014) Authors discuss various kinds of security issues and present a trust model to upgrade the security and interoperability of cloud computing condition. Authentication issue can be solved by utilizing digital signature and he recommended that information is encoded utilizing cryptography strategies in every cell of a table in cloud. At whatever point a client needs to make a question, the inquiry parameters are assessed against the information stored. The inquiry results are likewise decrypted by client not simply the cloud so it builds by large execution. Information Splitting is exceptionally quick when contrasted with encryption. The principle behind it is to part the information over various hosts that are non-communicable. To determine the issue of multi Tenancy, the authors recommended the cloud suppliers should utilize intrusion detection framework to protect their clients in cloud environment.

(Rao & Selvamani 2015) Authors recommended that Multi Tenancy licenses to store data by various customers on cloud servers there is a possibility of data intrusion. Exposures with data disengagement can be perceived or found using the tests, for instance, information approval and insecure storage. Authors propose encryption is better answer for secure data and avoid access of data from various customers, encoding applied on data that makes data totally unusable. To give better security high level of encryption methods can be used for putting away and recouping the data from cloud.

(Vurukonda & Rao 2016) Authors discuss different Cloud Storage issues like Data Privacy and integrity, Data Recoverability, Data Backup, Identity Management, Access Control and so on. According to them SecCloud protocol use encoding and decoding for storing the data in

protected mode. The cyclic added substance and groups of multiplicative matching is used for clients for their key generation. The Key Management alongside information integrity and protection are guaranteed by File Assured Deletion (FADE) Protocol. The SecCloud and FADE Protocol gives security, privacy and confidentiality yet don't give Data accessibility.

(Usman Jan and He 2016) Authors proposed a protected, lightweight, strong and effective plan for information interchange among the media clouds and mobile clients. The aim of this paper is to help real time formulating with power saving requirement. The purposed methodology is basically a mixture of PUK, SK and PRK and no requirement of consistent association between the clients. Authors examined the delay happening in the decryption procedure that can be limited next to receiver.

In this paper, high proficiency video coding related plan of encryption is discussed which is time effective, less unpredictable as far as calculations. The proposed plan encrypt the secret information in compressed space, not in encoding area and it comprises of different stages, which are information encryption, video encoding and decoding with or without interpreting. The analyzed plan attempts to maintain the visual nature of that video and keep the size of video stream same as before encryption process. Accordingly, it submits a perfect stage for continuous applications of video data. The secure information is conveyed in the form of encrypted video data so it is challenge for programmers to separate whole secure information. It is because of the way that programmers don't have the idea about the definite areas and examples of the hiding plan, regardless of whether they take the secret key.

(Aloraini & Hammoudeh 2017) Authors present a survey of the three fundamental information security characteristics with regards to cloud computing specifically accessibility, integrity and privacy. Authors give a technique for accomplish information confidenality and securing the data in cloud conditions utilizing RSA algorithm and steganography method yet in this including an additional layer of security includes more expense regarding time. With the assistance of Cramer-Shoup cryptosystem real objectives accomplish in key generation, encryption and decoding but in text messages only.

Authors proposed an arrangement which uses the HMAC algorithm to guarantee information reliability and random number secret key to give greater security. By far most of the information

secrecy arrangements in the cloud give static information storage approaches and don't examine the modification of these strategies. When downloading unique information, decode it, some strategies are authorized for encode the data before information is transferred once more. It's not a cheap procedure for huge information file.

(Singh, Nafis & Sethi 2017) Authors proposing a hybrid approach of RSA and SHA1 for improving the security. RSA is for encryption and decoding of the information and SHA1 is for creating hash value. It gives security which just the approved client can get to it. According to them before putting away the information into the cloud, it initially encodes the information. After receiving the request from the customer, CSP verifies the client and decrypts the message and conveys it to the client. Authors take a string and produce public and private key and encode the string utilizing RSA algorithm lastly creating the hash value of a similar message utilizing SHA1. In this, we selected the tool which requires highly skilled professionals and it is nearly costly.

(Jose & Christopher 2018) Authors proposed the technique for storing the message in e-learning storage framework with the help of data encryption standard and erasure code. With the help of this technique to encode the text and save it in the e-learning storage framework. Subsequent to encryption, the changed or new messages are stored in the cloud server farm. Authors talk about the Reed Solomon Code for encrypted messages. The proposed RS codes incorporates three parts like cloud controller, client and different nodes .The encoding plan that guarantee least number of data centers contrast with replication plot. Authors purposed successful method for transferring and downloading information with verified way in cloud related framework. It will expand the successful e-learning in cloud storage framework.

(Xiong & Shi 2018) Authors suggested the protection preservative contract out plan of flexible information hiding above encoded picture information in distributed computing and guarantees multimedia information security without depending on the dependability of cloud servers. Authors' purposed two reversible information hiding schemes like reversible data hiding and reversible information covering with homomorphic encryption in encoded space. Authors analyzed the flexible information hiding can be worked above the encoded picture at the various phases. This paper demonstrates the better execution in terms of capacity and security as contrast with existing arrangements.

(Abdulhamid, Sadiq, Abdullahi, Rana and Chiroma 2019) Authors bring the possibility of advancement of Blowfish encryption scheme that empowers them to encode their information before storage in the cloud. Authors considered and tested the created encoded application with ordinary measurements and contrast it with other scheme. The purposed plan is utilized for secure information storage in the public and business cloud computing condition. As per authors Blowfish acknowledged as toughest, highest speed and permit free algorithm and it produce an extraordinary key for encoding the message and similar key is utilized to recover the information from the cloud. They investigated the purposed calculation can't be utilized for records if size larger than 4GB due to its minor block size.

(Pachpor, N.N. and Prasad, P.S., 2018) Authors discussed some issues related to primary storage system in which the performance of large size file can be improved but when the size of the file from 4KB to 8KB then deduplication cannot improve the performance of the system. Author purposed some method related to performance oriented and reduce the traffic on the network. These methods are not capacity oriented but it improves the primary storage system.

(Kaur, R., Chana, I. and Bhattacharya, J., 2018) Authors discussed different types of deduplication like file level deduplication, block level deduplication. The deduplication applied on text, image and video data and improves the performance of the system. Author suggested that deduplication reduce overall storage cost, reduce storage space and improve the network bandwidth but this paper discuss some challenges related to deduplication like performance issue, small size files, optimization techniques.

(Tan, C.B., Hijazi, M.H.A., Lim, Y. and Gani, A., 2018) Cloud Storage has modern development for storing the data above the traditional storage system. Authors suggested some data integrity and accessibility methods for storing the data in cloud like proof of retrievability and provable data possession for ensuring the customer that their data will be in secure mode in the cloud like traditional storage system. Providing data integrity and accessibility with the help of these methods but they analyzed some challenges like finding the actual location of server where the information is stored. Geo location of the stored data, assured deletion and deduplication which are related to data storage still a challenge for cloud storage

.

3. Description of Broad Area

Cloud computing has turned out to be one of the most significant topic in today's time. Its advantages have pulled pretty much in every sector. In any case, so as to appreciate the wide usage of cloud computing services through wired/remote system, confirmation of cloud security as far as information privacy, validation, non-repudiation and integrity is a basic factor for its prosperity. Despite of all promotion about the cloud, enterprise clients are as yet hesitant to put their data in the cloud. Security and loss of control are the serious problems which reduce the development of distributed computing.

In spite of its focal points, the cloud computing framework faces extremely challenging task, particularly on reliability, information protection and security issues. As information is set on public clouds which are out of their confided in spaces, information proprietors don't have direct authority over their sensitive information and are stressed over potential information misfortune and additionally illicit utilization of their private information. As a rule, cloud servers are considered as inquisitive and untrusted; subsequently information proprietors hesitate to embrace cloud advancements as there are dangers of data exposure to the cloud specialist organization or an outsider. Along these lines, giving adequate security and security insurances is significant, particularly for applications handling government information, health information and financial system so on. Security is one the real worry about distributed computing which is by all accounts central point for the postponement in selection of its service. Cloud security, as characterized on Wikipedia, is "an evolving subdomain of computer security, network security and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing." Security and protection concerns are practically comparative over the conventional services and cloud services. The loss of authority over information is add on factor that enhances these worries and could prompt blunder of those information.

Distributed storage framework is an enormous scale circulated capacity worldview in which a pool of assets is accessible to clients. Cloud server is anything but difficult to use by the cloud customers. Accepting this is the situation, storage framework ought to satisfied CAP (Consistency, Availability, partition resistance) characteristics. Information stockpiling in the

cloud based framework is a procedure of putting away information by proprietor through distributed stockpiling specialist organization. At the hour of information storage, the security key issued for the unapproved access and taking care of information. Customer needs to get to the information from the cloud based framework; the cloud is required for the security key for opening the information. The clients send a solicitation for security key to the proprietor. Proprietor checked the approved or unapproved individual, and after that they provide the secure key. With quick improvement of cloud server farm, most of the associations will re-appropriate their assets for sharing in the cloud. To keep the information confidential against unknown cloud specialist co-ops, an incredible way is to store just encoded detrain a cloud. It shields the assets from unapproved customers. During the decoding, the key can be utilized by the client as demonstrated by the approval from the owner. Counting a few benefits and bad marks in information storage security in cloud based processing still a difficult task.

3.1 Gaps in the Research: Cloud storage has become modern development for storing the data over the traditional storing system which takes large storage space of data holder assets for backup and disaster retrieval purposes. But on the other side data owner does not have confidence on cloud storage and afraid to loosing confidentially of his critical data. Researcher found some techniques to provide security of the data with confidentially, data integrity and availability when client store it in the cloud with the help of proof of retrievability but there are some gaps in their research like:

- Geo location visibility of outsourced stored data not available with owner.
- Owner does not have confidence on assured deletion of his data and afraid of retrieval of his confidential data by someone, post deletion.
- Duplicate copy of data in cloud having risk of data leakage and threat on data confidentiality.
- High resource cost to afford client-side encryption to maintain data confidentiality.

4. Objectives

1. To examine the pros and cons of existing encryption algorithms for storage of data in cloud
2. To review the importance of deduplication in enhancing cloud storage in cloud.
3. To design and develop a novel approach for storing image data in Cloud.
4. To implement the approach and test the developed algorithm on a real time data set.
5. To compare the performance of the proposed algorithm with that of the existing encryption schemes.

5. Methodology

1. Literature Review
2. Study of accessible instruments, components, sorting issues and difficulties, assessing disadvantages of existing frameworks and identifying zones of act of improvisation to make cloud adoption become more agreeable to the clients.
3. Formulating the research objectives- The Problem explanation.
4. Identifying the available tools to simulate the existing data integrity schemes and developing better solution.
5. Design and development of an improved security mechanism in a simulated environment to secure the data storage.
6. Research publications dependent on the exploration work, writing of thesis and submission.

6. Expected Outcome of the Research

Cloud computing is a buzz word now a days but organizations are still sometimes reluctant to outsource their data to cloud. One of the major concerns is security and integrity of the stored data. The research work will provide insight knowledge of the current data integrity scheme for cloud storage. It also helps to compare the different mechanism and their merits and demerits. The research work will come out with an efficient security mechanism for data storage in cloud. The research work will be to design an efficient deduplication scheme to minimize risk of data loss and encryption scheme to ensure data integrity for data storage.

7. References

Aloraini, A. and Hammoudeh, M., 2017, July. A survey on data confidentiality and privacy in cloud computing. In Proceedings of the International Conference on Future Networks and Distributed Systems (pp.1-7).

An, Y.Z., Zaaba, Z.F. and Samsudin, N.F., 2016, November. Reviews on security issues and challenges in cloud computing. In IOP Conference Series: Materials Science and Engineering (Vol. 160, pp.1-9).

Azougaghe, A., Kartit, Z., Hedabou, M., Belkasmi, M. and El Marraki, M., 2015, December. An efficient algorithm for data security in cloud storage. In 2015 15th International Conference on Intelligent Systems Design and Applications (ISDA) (pp. 421-427).

Bhandari, A., Gupta, A. and Das, D., 2016, January. Secure algorithm for cloud computing and its applications. In 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence) (pp. 188-192).

Chen, K. and Xu, D., 2018. An efficient reversible data hiding scheme for encrypted images. International Journal of Digital Crime and Forensics (IJDCF) (Vol.10, pp.1-22).

Cyril, B.R. and Kumar, D.S.B.R., 2015. Cloud computing data security issues, challenges, architecture and methods-a survey. Int. J. Eng. Technol (Vol.2,pp.848-857).

Hashizume, K., Rosado, D.G., Fernández-Medina, E. and Fernandez, E.B., 2013. An analysis of security issues for cloud computing. Journal of internet services and applications (Vol. 4, pp.1-13).

Hussain, I. and Ashraf, I., 2014. Security issues in cloud computing-a review. International Journal of Advanced Networking and Applications (Vol. 6, pp.2240-2243).

Jose, G.S.S. and Christopher, C.S., 2018. Secure cloud data storage approach in e-learning systems. Cluster computing (pp.1-6).

Kaur, R., Chana, I. and Bhattacharya, J., 2018. Data deduplication techniques for efficient cloud storage management: a systematic review. The Journal of Supercomputing, (Vol.74, pp.2035-2085).

Li, Y., Gai, K., Qiu, L., Qiu, M. and Zhao, H., 2017. Intelligent cryptography approach for secure distributed big data storage in cloud computing. Information Sciences (Vol.387, pp.103-115).

Mahalle, V.S. and Shahade, A.K., 2014, October. Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm. In 2014 International Conference on Power, Automation and Communication (INPAC) (pp. 146-149).

Mahmood, Z., 2011, September. Data location and security issues in cloud computing. In 2011 International Conference on Emerging Intelligent Data and Web Technologies (pp. 49-54).

Ng, W.K., Wen, Y. and Zhu, H., 2012, March. Private data deduplication protocols in cloud storage. In Proceedings of the 27th Annual ACM Symposium on Applied Computing (pp. 441-446).

Ouedraogo, M., Mignon, S., Cholez, H., Furnell, S. and Dubois, E., 2015. Security transparency: the next frontier for security research in the cloud. Journal of Cloud Computing (Vol. 4, pp.1-14).

Pachpor, N.N. and Prasad, P.S., 2018, March. Improving the Performance of System in Cloud by Using Selective Deduplication. In 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 314-318).

Rao, B.T., 2016. A study on data storage security issues in cloud computing. Procedia Computer Science(Vol. 92, pp.128-135).

Rao, R.V. and Selvamani, K., 2015. Data security challenges and its solutions in cloud computing. Procedia Computer Science(Vol.48, pp.204-209).

Rawal, B.S., Vijayakumar, V., Manogaran, G., Varatharajan, R. and Chilamkurti, N., 2018. Secure disintegration protocol for privacy preserving cloud storage. Wireless Personal Communications(Vol.103, pp.1161-1177).

Sadiq N.A., Abdullahi, M., Rana, N., Chiroma, H. and Dada, E.G., 2018. Development of Blowfish Encryption Scheme for Secure Data Storage in Public and Commercial Cloud Computing Environment. I-manager's Journal on Cloud Computing(Vol.5,pp.1-10).

Singh, S., Scholar, M.T., Nafis, T. and Sethi, A., 2017. Cloud Computing: Security Issues & Solution (Vol.13, pp.1419-1429).

Sun, Y., Zhang, J., Xiong, Y. and Zhu, G., 2014. Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks(Vol. 10, pp.1-9).

Suresh, G.V.A.P.K., 2019. Data Sharing With CP-ABE to Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage(pp.620-623).

Tan, C.B., Hijazi, M.H.A., Lim, Y. and Gani, A., 2018. A survey on Proof of Retrievability for cloud data integrity and availability: Cloud storage state-of-the-art, issues, solutions and future trends. Journal of Network and Computer Applications (Vol. 110, pp.75-86).

Usman, M., Jan, M.A. and He, X., 2017. Cryptography-based secure data storage and sharing using HEVC and public clouds. Information Sciences (Vol. 387, pp.90-102).

Xiong, L. and Shi, Y., 2018. On the privacy-preserving outsourcing scheme of reversible data hiding over encrypted image data in cloud computing. Computers, Materials & Continua (Vol. 55, pp.523-539).

Zhang, G., Wang, T., Wang, G., Liu, A. and Jia, W., 2018. Detection of hidden data attacks combined fog computing and trust evaluation method in sensor-cloud system. Concurrency and Computation: Practice and Experience(pp.1-13).

Zhao, J., Mortier, R., Crowcroft, J. and Wang, L., 2018, December. Privacy-preserving machine learning based data analytics on edge devices. In Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society (pp. 341-346).

Zhe, D., Qinghong, W., Naizheng, S. and Yuhan, Z., 2017, May. Study on data security policy based on cloud storage. In 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids)(pp. 145-149).

SYNOPSIS PRONIKA NOV.15,2019

ORIGINALITY REPORT

Excluding matches less than 14 words

4%	3%	3%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.imanagerpublications.com Internet Source	1%
2	Submitted to Campbellsville University Student Paper	1%
3	www.ijeast.com Internet Source	<1%
4	Tan Choon Beng, Mohd Hanafi Ahmad Hijazi, Yuto Lim, Abdullah Gani. "A survey on Proof of Retrievability for cloud data integrity and availability: Cloud storage state-of-the-art, issues, solutions and future trends", Journal of Network and Computer Applications, 2018 Publication	<1%
5	"Big Data Analytics", Springer Science and Business Media LLC, 2018 Publication	<1%
6	Submitted to University of Maryland, University College Student Paper	<1%

Dr. [illegible]
University Librarian
Central Library
Manav Rachna International
Institute of Research & Studies
Faridabad

Scanned with CamScanner

7	Submitted to Victoria University Student Paper	<1%
8	"Advanced Informatics for Computing Research", Springer Nature, 2019 Publication	<1%
9	Kaiping Xue, Weikeng Chen, Wei Li, Jianan Hong, Peilin Hong. "Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage", IEEE Transactions on Information Forensics and Security, 2018 Publication	<1%
10	Submitted to Monash University Student Paper	<1%

Exclude quotes	On	Exclude matches	< 14 words
Exclude bibliography	On		

Scanned with CamScanner